REMARKS

Claims 1, 5-7, 13, 15-16, 19-21, 27, and 29-30 are pending. Claims 1, 7, 13, 15, 16, 21, 27, and 29 have been amended and claims 2-4, 8-12, 14, 17, 18, 22-26, 28, and 31-34 have been canceled. No new matter has been introduced. Reexamination and reconsideration of this application is respectfully requested.

In the April 7, 2004 Office Action, the Examiner rejected claims 1-34 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,401,206 to Khan ("the Khan reference"). These rejections are respectfully traversed.

Embodiments of the present invention are directed to a system and method of creating and using strong passwords with high entropy. The system and method utilize user generated questions and answers. To protect against an adversary obtaining the questions and answers, multiple levels of questions and answers are used. The user is first presented with a page containing fields for entering answers to a plurality of questions and a field for entering a "retrieval answer". At this stage, the plurality of questions are not displayed, nor is the question displayed for the "retrieval answer". If the user can enter the correct answers without the questions being displayed, then this step is done and the user may access the information that is otherwise protected. However, if the user needs to see the plurality of questions first, then the user must enter the correct "retrieval answer" in the field labeled as such. If the user cannot enter the "retrieval answer" without seeing the "retrieval question" then the user must ask to see the "retrieval question." If the user so requests, the "retrieval question will be displayed, so that the user can then enter the retrieval answer to display the plurality of questions. However, to prevent unauthorized access, anytime someone asks to display

the retrieval question, a notification is sent to the user alerting him to the fact that the retrieval question has been requested. Thus, if it was not the user that requested the retrieval question, the user will know someone else is attempting to access the information and may change the retrieval question or take other defensive measures. For other safety purposes, the actual answers are not stored on the remote server, and instead only a hashed answer (a concatenation of the plurality of answers that have been encrypted) is stored on the remote server. Thus, even if someone has access to the remote server, they still will not be able to decipher the answers to the plurality of questions. Claim 1, as amended, recites: A method of creating a strong pass phrase, the method comprising:

obtaining a plurality of questions and a plurality of answers corresponding to the plurality of questions;

combining the plurality of answers into a single pass phrase, wherein the plurality of answers are concatenated together with a fixed random value and a cryptographic hash function is applied to the concatenation to create a hashed answer;

storing the hashed answer on a remote server without storing the plurality of answers on the remote server; and

obtaining a retrieval question and a retrieval answer, the retrieval answer being used to display the plurality of questions.

The Khan reference is directed to a portable digital identity that includes personal information and may include data representing the person's handwritten signature and one or more passwords. The digital identity optionally includes data representing seals, fingerprints and biometric information. The digital identity can be

used to bind a verifiable electronic impression with an electronic document using electronic watermarks so that any modification in the document or electronic impression bound to the document may be detected.

The Khan reference does not teach, suggest, or disclose, a method of obtaining a strong password including *storing the hashed answer on a remote server without storing the plurality of answers on the remote server and obtaining a retrieval question and a retrieval answer, the retrieval answer being used to display the plurality of questions*, as recited by independent claim 1, as amended.

Firstly, the Khan reference does not teach, suggest, or disclose storing the hashed answer (which is a concatenation of the plurality of answers subjected to an encryption scheme), without storing the actual answers on the remote server. The concatenation of the plurality of answers subjected to an encryption scheme makes for a password of very high entropy. The password is very difficult to break. Storing only that hashed answer and not the answers themselves means that even those individuals with access to the remote server would be unable to decipher the actual answers to the plurality of questions. The Khan reference does not teach, suggest, or disclose such protective measures and thus Applicant believes that claim 1, as amended, overcomes the cited art.

Secondly, the Khan reference does not teach suggest or disclose the use of a retrieval answer necessary to display the plurality of questions to which the answers form the pass phrase (password). In the present invention, a user is first presented with a page having the fields for a plurality of answers. However, the questions for those answers are not displayed immediately. If the user needs the plurality of questions

before he can provide the plurality of answers, then the user must provide a "retrieval answer." If the user does not need the plurality of questions to provide the answers, the user does not need to input the retrieval answer.

Original dependent claim 11 (now canceled) recited a similar limitation. It read: "The method of claim 10, further comprising requiring a retrieval pass phrase before the remote server will release the plurality of pass phrase questions, wherein the retrieval pass phrase is pre-stored in the remote server and is formed from a set of retrieval answers previously entered by a user." The Examiner rejected claim 11 stating that the Khan reference anticipated the claim at Column 12, lines 49-63. That section of Khan reads:

> "In case the device on which the user's digital identity resides is lost, the unique personal identifiers 1 and 2 can be fully recovered as long as the signer maintains his long term memory. This can be done by taking the custom questions out of the public components of the digital identity available from any previously signed document, and repeating the entire digital identity creation process, which implies that the user must remember the answers to all the questions he used in the original identity. The reconstructed identity will contain personal identifiers 1 and 2 that will be exact matches of that contained in the original digital identity. These identifiers can be used for verification of identity marks for detection of forgeries (when the public key cryptographic assumption is broken or the private key is stolen.)"

The Applicant is confused as to where this passage states that a retrieval answer will be needed before the plurality of questions will be provided. In fact, the only thing this passage states is that if the user's computer or computer media storing the user's digital identity is lost or stolen, the user will have to repeat the entire set up process again using the answers to the same questions that he had before. That is not the same as using a "retrieval answer" to retrieve the plurality of questions which must be answered to obtain the pass phrase (password). Thus Applicant is of the belief that the

rejection to claim 11 should have been withdrawn. However, claim 11 has been canceled and the limitations of the claim have been incorporated into claim 1. Thus, Applicant believes that the rejection to claim 1, as amended, should be withdrawn.

Likewise, the Examiner rejected dependent claim 13 based on a section in Khan which the Applicant does not believe anticipates the claim. Claim 13, as amended, reads: The method of claim 7, wherein a user is notified if anyone asks for the retrieval question. The Examiner rejected claim 13 based on Column 9, lines 66-67 and Column 7, lines 1-13 of Khan.

These passages read:

> Column 9, lines 66-67: "The identity marks can be used to detect forgeries as discussed below."
>
> Column 7, lines 1-13: "The system then generates a public/private key pair (4008). The private key 4010 will be maintained with the digital identity, whereas the public key 4009 will be presented to a certification authority for publishing.
> A user's "digital identity" in a preferred embodiment includes the user name obtained at step 4001; the public information obtained at step 4002; and private information obtained in steps 4003-4004; the personal questions and answers obtained in steps 4005 and 4006; the public/private key pair generated at step 4008; the handwritten signature and/or other biometric parameters obtained at step 4007; and personal identifiers 1, 2, and 3."

The Applicant is confused because no where in those passages does it state that a user will be notified if someone requests his retrieval question. These passages do not mention a retrieval question or its equivalent (in fact no where in the entire patent is a retrieval question mentioned). These passages don't mention notifying the user. Nothing in these passages teaches, suggests, or discloses anything close to the limitation recited in claim 13. Thus Applicant believes the rejection to claim 13 should be withdrawn.

Additionally, the rejection of claim 29 is not understood. Claim 29 reads: A client workstation comprising:

a processor;

a display connected to the processor;

a computer memory connected to the processor, the computer memory including:

a viewing program for rendering information received from a server on the display, the display displaying a plurality of fields for entering a plurality of pass phrase answers *and an option for requesting a plurality of pass phrase questions corresponding to the plurality of the pass phrase of answers*, and

a client program for combining the pass phrase answers to form a single pass phrase,

wherein if the option for requesting the set of the pass phrase questions is chosen, a field for entering a retrieval answer and an option for requesting a retrieval question corresponding to the retrieval answer is displayed.

The Examiner stated that claim 29 was rejected based on Khan, column 12, lines 1-18. That passage states:

> FIG. 9 depicts the modifications made in the verification process. The modifications required include separation box 7301 that separates the document from identity marks (7003) and public components of the digital identity (7302). The serial numbers, positional information and time-stamp/random information are validated by comparing them with information stored in a database. When the conventional digital signature attached to the document is validated and the time-stamp or random number attached to a document is validated, the binding of the electronic impression made by a digital identity with the document is deemed authentic and the decrypted document is then displayed along with some of the information in the public components of a digital identity. In this embodiment, the handwritten signature or seal or photographic image or

biometric part of the digital identity is displayed with the document to indicate that the document was indeed signed with the digital identity. The separated identity marks can be used for additional verification as described in the explanation of FIG. 7.

The Applicant cannot find anywhere in this passage where mention is made of *an option for requesting a plurality of pass phrase questions corresponding to the plurality of the pass phrase of answers*, nor where there is any mention of *if the option for requesting the set of the pass phrase questions is chosen, a field for entering a retrieval answer and an option for requesting a retrieval question corresponding to the retrieval answer is displayed.* The Examiner is respectfully requested to point out where such limitations are taught. In the alternative, the Examiner is requested to withdraw the rejection of claim 29.

Claims 7, 15, 21 and 29 all recite limitations similar to independent claim 1 as amended. Thus Applicant requests that the rejections of such claims be withdrawn for the same reasons as for claim 1. Claims 5-6 all depend directly or indirectly from independent claim 1, and thus Applicant requests that the rejections of these claims be withdrawn for the same reasons as for claim 1. Claims 13 depends directly from independent claim 7, and thus Applicant requests that the rejection of this claim be withdrawn for the same reasons as for claim 7. Claims 16 and 19-20 all depend directly or indirectly from independent claim 15, and thus Applicant requests that the rejections of these claims be withdrawn for the same reasons as for claim 13. Claim 27 depends directly from independent claim 21, and thus Applicant requests that the rejection of this claim be withdrawn for the same reasons as for claim 21. Claim 30 depends directly from independent claim 29, and thus Applicant requests that the rejection of this claim

be withdrawn for the same reasons as for claim 29.

Applicant believes that the foregoing amendments place the application in condition for allowance, and a favorable action is respectfully requested. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles telephone number (213) 488-7100 to discuss the steps necessary for placing the application in condition for allowance should the Examiner believe that such a telephone conference would advance prosecution of the application.

Respectfully submitted,

PILLSBURY WINTHROP LLP

Date: June 24, 2004

By: _____
Roger R. Wise
Registration No. 31,204
Attorney For Applicant

725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Telephone: (213) 488-7100
Facsimile: (213) 629-1033